FortiClient Rebranding Tool

The licensed FortiClient Rebranding Tool is used to create custom FortiClient installation files and rebrand FortiClient. Starting with FortiClient 5.6.0, a Site Toolkit subscription to Fortinet Developer Network (https://fndn.fortinet.net/) is required to access the licensed tool. Although you can use the tool in trial mode, a license key is required to access all of the features available with the tool.

The FortiClient Rebranding Tool is available for Microsoft Windows and Mac OS X operating systems.

Overview

Following is an overview of using the FortiClient Rebranding Tool:

1. Prepare to download the subscription-based tool. See Preparing to download and license the tool on page 1.
2. Log into your FNDN account, add the activation code, and download the tool from FNDN. See Downloading the tool on page 2.
3. (Optional) Prepare configuration files and Telemetry gateway IP lists. See Preparing configuration files on page 2.
   You have the option to add a FortiClient configuration file and/or Telemetry gateway IP list to the FortiClient installer. Before you create the installer, you should get these files ready for selection.
4. Create a custom FortiClient installer. See Creating custom FortiClient installation files on page 5.
   You will load the license key when you use the tool.
5. (Optional) Rebrand the FortiClient installer. See Rebranding FortiClient on page 15.
6. Deploy the custom FortiClient installation packages. See Deploying custom FortiClient installation packages on page 28.

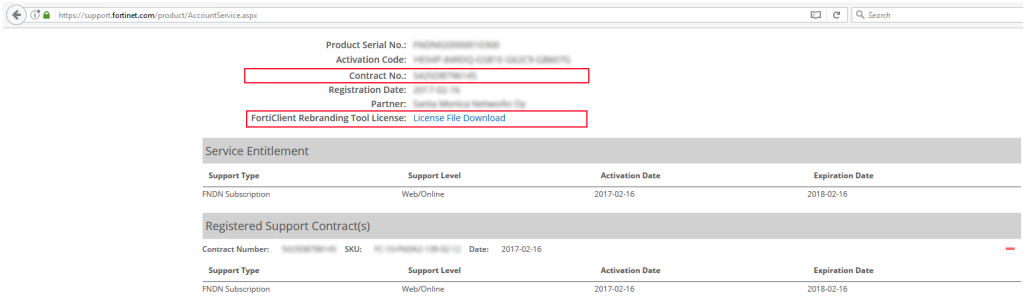
Preparing to download and license the tool

You must perform a number of tasks to access the FortiClient Rebranding Tool on FNDN.

To prepare to download and license the tool:

1. Purchase a Site Toolkit subscription to FNDN. Contact your Fortinet sales representative.
   A contract number for FNDN is generated. The contract number is included in the material that you receive for the purchase.
2. Register the contract number for FNDN with Fortinet Customer Service & Support at https://support.fortinet.com/.
   The registration process generates the following items:
   - Activation code for FNDN
   - License key file for FortiClient Rebranding Tool

You can retrieve the items from your account.



3. On the Fortinet Customer Service & Support site (https://support.fortinet.com/), go to *Asset* > *View Account Service* > *FNDN*, and download the license key from your account. You will add it to the FortiClient Rebranding Tool later.

   Place the license key in an easily accessible location. Because the FortiClient Rebranding Tool is not installed on the management computer, you must upload the license key each time that you run the tool to create a custom FortiClient installer. See Creating custom FortiClient installation files on page 5.
4. Copy the activation code for FNDN. You will add it to your FNDN account later.

Downloading the tool

Download the licensed FortiClient Rebranding Tool from the Fortinet Developer Network site.

A Site Toolkit subscription to FNDN and an account to FNDN are required to access and download the FortiClient Rebranding Tool. See Preparing to download and license the tool on page 1.

To download the tool:

1. Log into your FNDN account at https://fndn.fortinet.net/.

   If you do not have an account for FNDN, you must create an account at https://fndn.fortinet.net/index.php?/register/.

   When you create an FNDN account, you are required to include the email address for two Fortinet sponsors. Fortinet sponsors are Fortinet employees who can verify that you are a Fortinet customer. Contact your sales representative or sales engineer for email addresses for Fortinet sponsors.
2. Add the activation code from your Fortinet Customer Service & Support at https://support.fortinet.com/ to your FNDN account settings.
3. Go to the *Tools* tab, and download the FortiClient Rebranding Tool.

Preparing configuration files

You can select the following types of files in the FortiClient Rebranding Tool when you create a custom FortiClient installer:

- Configuration file
- Gateway IP list

This section describes how to retrieve and edit the files to prepare them for use with the FortiClient Rebranding Tool.

You can use an XML editor to make changes to the FortiClient configuration file and Telemetry gateway IP list. For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library at http://docs.fortinet.com.

Retrieving FortiClient configuration files

You can retrieve a configuration file from FortiClient console. The configuration file contains the settings for FortiClient. After you retrieve the configuration file, you can use an XML editor to make changes to the configuration file. Then you can select the FortiClient configuration file in the FortiClient Rebranding Tool.

To retrieve FortiClient configuration files:

1. In FortiClient console, go to *Settings*.
2. In the *System* area, click *Backup*.
3. Select a destination, and click *OK*.

Configuring Telemetry gateway IP lists

You can retrieve a configuration file from FortiClient console to access the XML elements for the Telemetry gateway IP list.

If you are using FortiClient EMS (Enterprise Management Server), you can export a gateway IP list from FortiClient EMS. See the *FortiClient EMS Administration Guide*.

The Telemetry gateway IP list contains IP addresses for FortiGate and/or FortiClient EMS. FortiClient uses the Telemetry gateway IP list to connect FortiClient Telemetry to FortiGate or FortiClient EMS.

After you retrieve the configuration file, you can use an XML editor to locate the elements for the Telemetry gateway IP list and modify them.

To configure Telemetry gateway IP lists:

1. In FortiClient console, retrieve the configuration. See Retrieving FortiClient configuration files on page 3.
2. Open the configuration file in an XML editor.
3. Remove all elements, except the elements needed to configure the Telemetry gateway IP list. See Example XML of Telemetry gateway IP list on page 5.
4. Add IP addresses to the configuration file by using an XML editor.
   When using only FortiGate for endpoint control, use the `<fortigate>` element to identify one or more IP addresses for FortiGate devices.

When using FortiGate integrated with EMS, use the <fortigate> element to identify one or more IP addresses for FortiGate devices, and use the <notification_server> element to identify the IP address for EMS.

5. Save the configuration file.

Example XML of Telemetry gateway IP list

Following is an example XML file for a Telemetry gateway IP list. In this example, endpoints will connect Telemetry to FortiGate by using the IP addresses in the <fortigate> element and send notifications to FortiClient EMS by using the <notification_server> element.

```
<?xml version="1.0" encoding="UTF-8" ?>
   <forticlient_configuration>
      <endpoint_control>
         <enabled>1</enabled>
         <disable_unregister>0</disable_unregister>
         <silent_registration>1</silent_registration>
         <fortigates>
            <fortigate>
               <serial_number>fgt_sn0</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     da7e6495841d8fc9c61067f81ef4cac01d697bb7e160c24d</registration_password>
               <addresses>172.30.254.150:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn1</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     6c9f088323beef31ea969c1c31c6db0e766273cb21851e68</registration_password>
               <addresses>172.30.254.174:8013</addresses>
            </fortigate>
            <fortigate>
               <serial_number>fgt_sn2</serial_number>
               <name>fgt_name</name>
               <registration_password>Enc
                     7e819fa80a68ca2b602fdad54ba76190f03777c70399471d</registration_password>
               <addresses>172.30.254.158:8013</addresses>
            </fortigate>
            <notification_server>
               <address>us-ems1.myfortinet.com:8013</address>
            </notification_server>
         </fortigates>
      </endpoint_control>
   </forticlient_configuration>
```

Creating custom FortiClient installation files

The following section provides instructions on creating a custom installer file using the FortiClient Rebranding Tool.

You have the option to select a FortiClient configuration file and/or Telemetry gateway IP list when you create a custom FortiClient installer. See Preparing configuration files on page 2.

Ensure that you select all modules in the FortiClient installer that you want installed on endpoints. To enable other features after FortiClient is installed, you must uninstall FortiClient from endpoints, and reinstall an MSI file with the desired features included in the FortiClient installer.

If you're using FortiClient EMS to deploy and manage FortiClient endpoints, you can create a FortiClient installer that includes most or all modules, and you can use a profile from FortiClient EMS to disable and enable modules without uninstalling and reinstalling FortiClient.

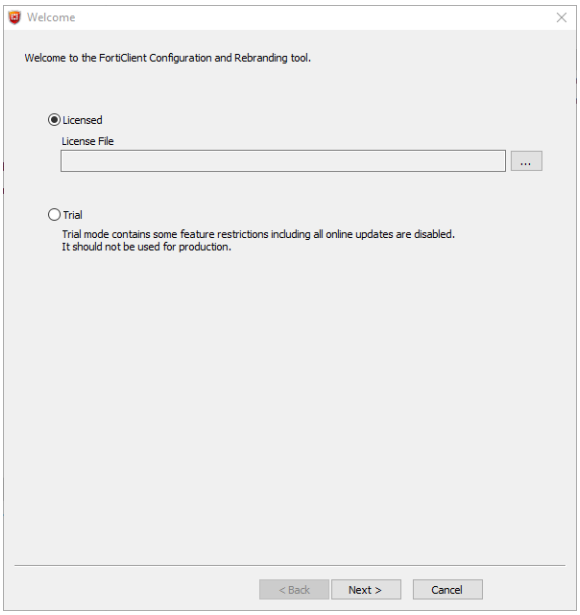
The FortiClient Rebranding Tool is not installed on the management computer. You must upload the license key file (.lic) each time you run the tool.

Using FortiClient Rebranding Tool for Windows

Windows has a hard limit of 260 characters on file path length. It is recommended to run the FortiClient Rebranding Tool in a shallow directory structure, such as c:\temp\, to avoid hitting the hard limit.

To create a custom FortiClient installation file:

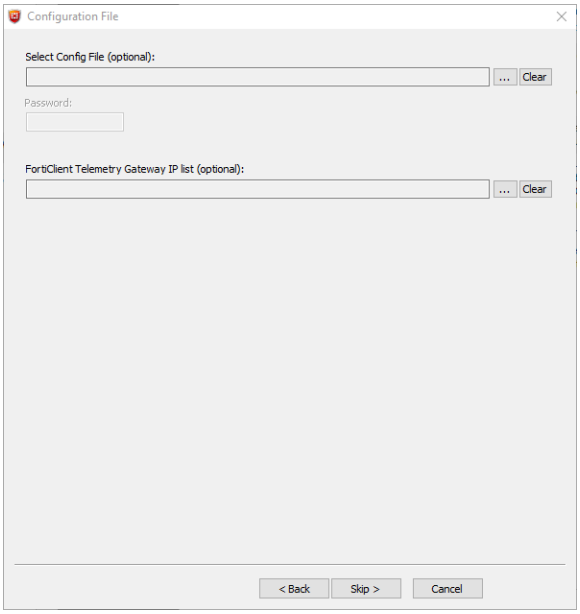
1. Double-click the *FortiClientRebrandingTool.exe* application file to launch the tool.
   The *Welcome* page displays with the following options:



Licensed	Select to use the tool in licensed mode. Licensed mode requires a FortiClient Rebranding Tool license key. See Preparing to download and license the tool on page 1.
Trial	Select to use the tool in trial mode. In trial mode, all online updates are disabled and VPN connections are time-limited. The trial installer is intended to be deployed in a test environment.

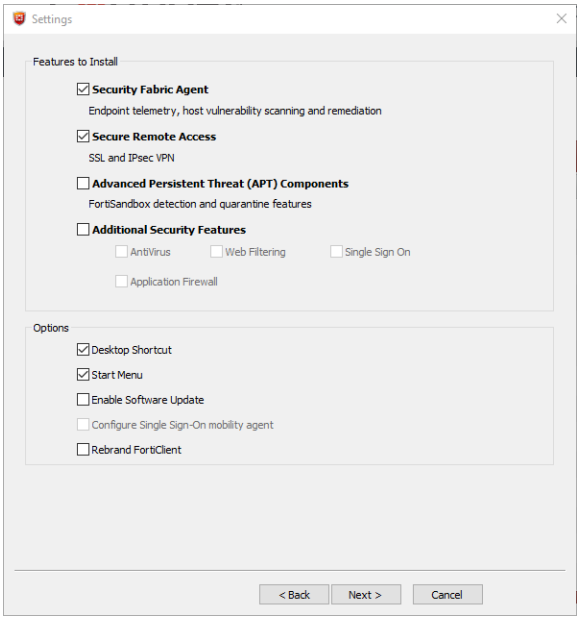
2. Click the *Licensed* radio button, and click the *Browse* button.
3. Locate and select the license key, and click *Next*.

4. The *Configuration File* page displays with the following options.



Select Config File (optional)	Select a FortiClient configuration file (`.conf`, `.sconf`) to include in the installer file.
Password	If the FortiClient configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
FortiClient Telemetry Gateway IP List (optional)	Select a FortiClient Telemetry gateway IP list to include in the installer file. This option is disabled when using Trial mode.

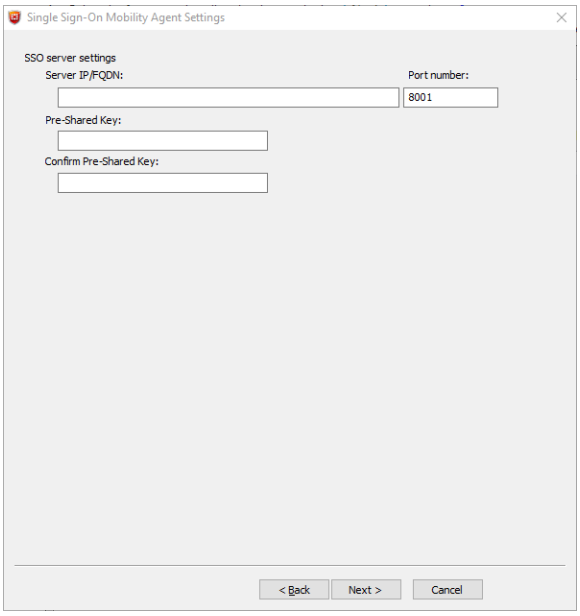
Locate and select the FortiClient configuration file on your management computer, and click *Next*. If you do not want to include settings from a configuration file, click *Skip* to continue. The *Settings* page displays.



The following options are available for custom installations:

Features to Install		
	Security Fabric Agent	Selected by default to support Fortinet Security Fabric. FortiClient Telemetry is always installed to support integration of FortiClient into the Security Fabric as follows: • Participate in compliance • Send user ID, avatar, and email address to FortiGate • Be managed by EMS Along with the Vulnerability Scan component (also included in this agent), this provides the Security Fabric administrators an overview of the endpoint state. Clear the checkbox to exclude the *Compliance* and *Vulnerability Scan* tabs from the FortiClient installation file.
	Secure Remote Access	Select to include SSL and IPsec VPN modules in the FortiClient installation file.
	Advanced Persistent Threat (APT) Components	Select to include FortiSandbox detection and quarantine modules in the FortiClient installation file.
	Additional Security Features	Select to include one or more of the following modules in the FortiClient installation file: • AntiVirus • Web Filtering • Single Sign On • Application Firewall
Options		
	Desktop Shortcut	Select to create a FortiClient desktop icon on the endpoint.
	Start Menu	Select to add FortiClient to the start menu on the endpoint.
	Enable Software Update	Select to enable FortiClient software updates via FortiGuard Distribution Network on endpoints. This option is disabled when *Rebrand FortiClient* is selected. This option is also disabled when using trial mode.
	Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator. You must select the *Single Sign On* checkbox in the *Features to Install* area first. This option is disabled when using trial mode.
	Rebrand FortiClient	Select to rebrand FortiClient. When selected, the option to enable software update is not available.

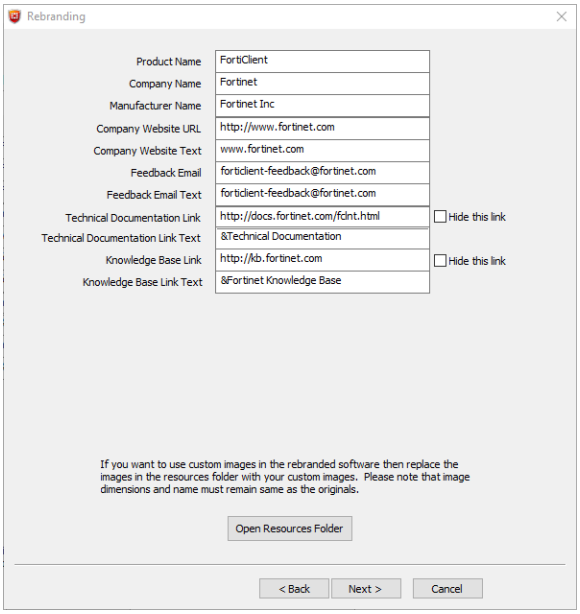
5. Select the features to install and options, and click *Next* to continue.
   If you selected the *Configure Single Sign-On mobility agent* checkbox, the *Single Sign-On Mobility Agent Settings* page displays.



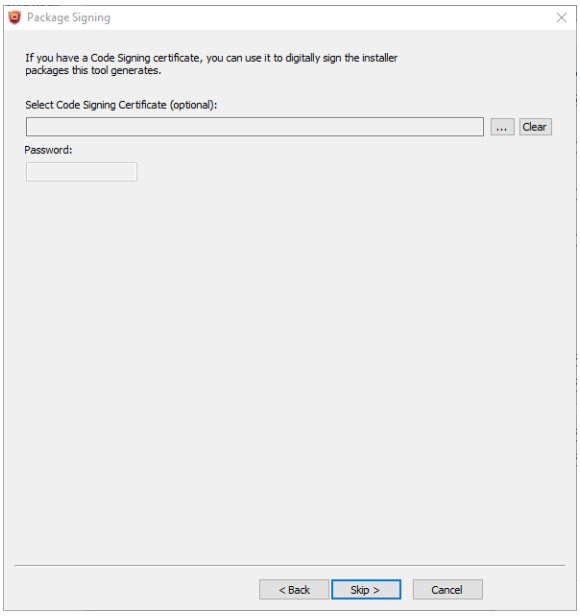
6. Configure the following settings:

Server IP/FQDN	Enter the FortiAuthenticator server's IP address or FQDN.
Port number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

7. Select *Next* to continue.
   If you selected to rebrand FortiClient, the *Rebranding* page is displayed.



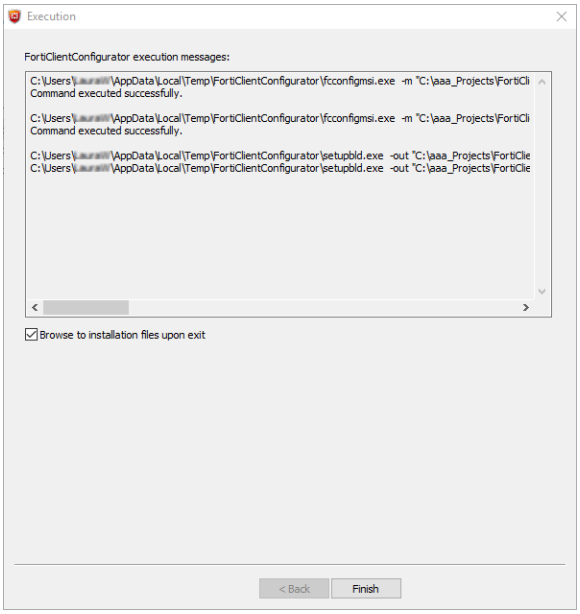
8. Rebrand FortiClient elements as required. The resources folder contains graphical elements.
9. Click *Next* to continue. The *Package Signing* page displays.



10. Configure the following settings:

Select Code Signing Certificate (optional)	If you have a code signing certificate, you can use it to digitally sign the installer package this tool generates.
Password	If the certificate file is password protected, enter the password.

11. (Optional) Browse and select the code signing certificate on your management computer. If you do not want to digitally sign the installer package, select *Skip* to continue. The *Execution* page displays.



This page provides details of the installer file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

12. When you click *Finish*, the folder containing the newly created MSI file will open when the *Browse to installation files upon exit* checkbox is selected.

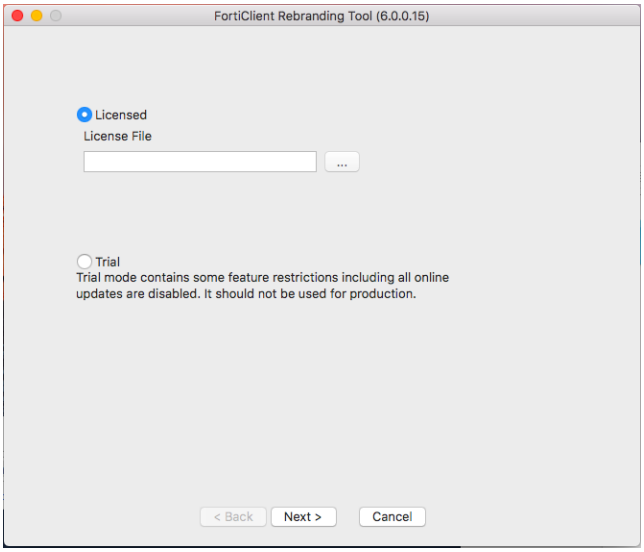
Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly. An `.exe` installation file is created for manual distribution.

Installation files are organized in folders within the folder where you placed the *.exe* file for the FortiClient Rebranding Tool. Folder names identify the type of installation files that were created and the creation date.

Using FortiClient Rebranding Tool for Mac OS X

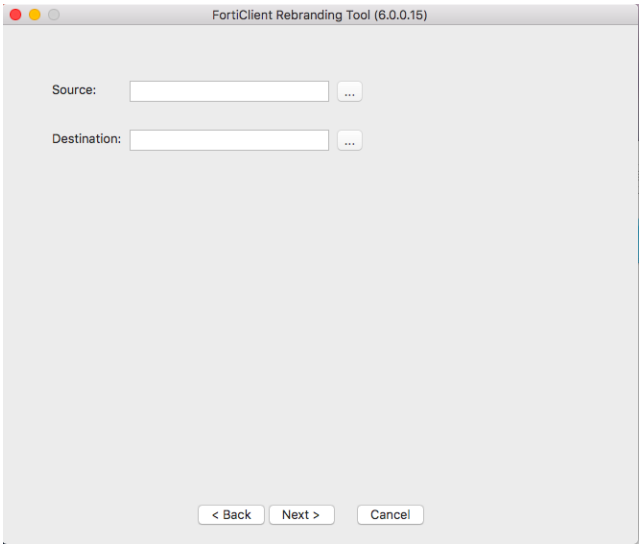
To create a custom FortiClient installation file:

1. Double-click the FortiClientRebradingTool_6.0.0.xxxx.dmg application file, and double-click the FortiClientRebrandingTool icon to launch the tool.
2. Configure the following settings, and click *Next*:



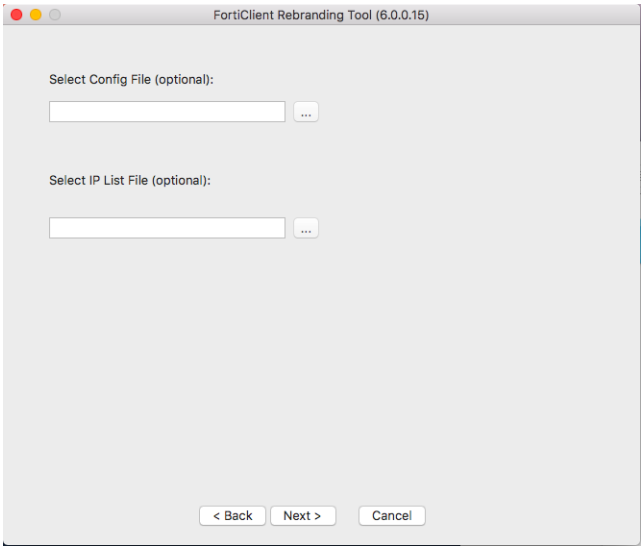
Licensed	Select to use the tool in licensed mode. Licensed mode requires a FortiClient Rebranding Tool license key. See Preparing to download and license the tool on page 1.
Trial	Select to use the tool in trial mode. In trial mode, all online updates are disabled and VPN connections are time-limited. The trial installer is intended to be deployed in a test environment.

3. Configure the following settings, and click *Next*:



Source	Select the FortiClient Installer file on your management computer. You must use the full installer file, otherwise FortiClient Rebranding Tool will fail to create a custom installation file. The FortiClient Installer version and FortiClient Rebranding Tool version must match, otherwise the Configurator will fail to create a custom installation file.
Destination	Enter a name for the custom installation file and select a destination to save the file on your management computer.

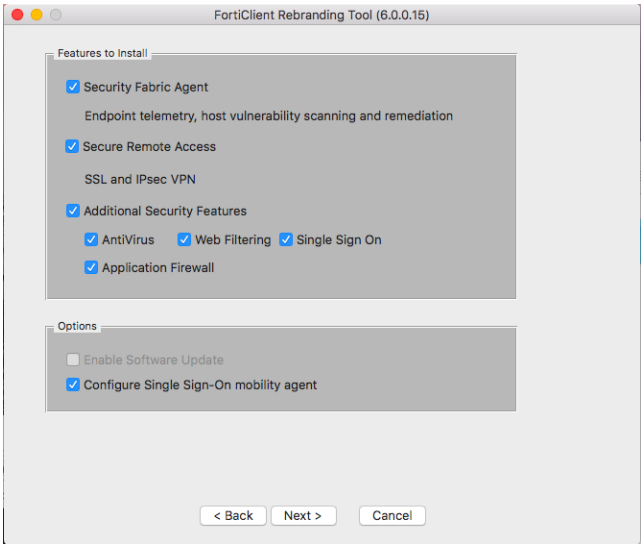
4. (Optional) Configure the following settings, and click *Next*:



Select Config File (optional)	Select a FortiClient configuration file (`.conf`, `.sconf`) to include in the installer file.

Password	If the FortiClient configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.
Select IP List File (optional	Select a FortiClient Telemetry gateway IP list to include in the installer file.

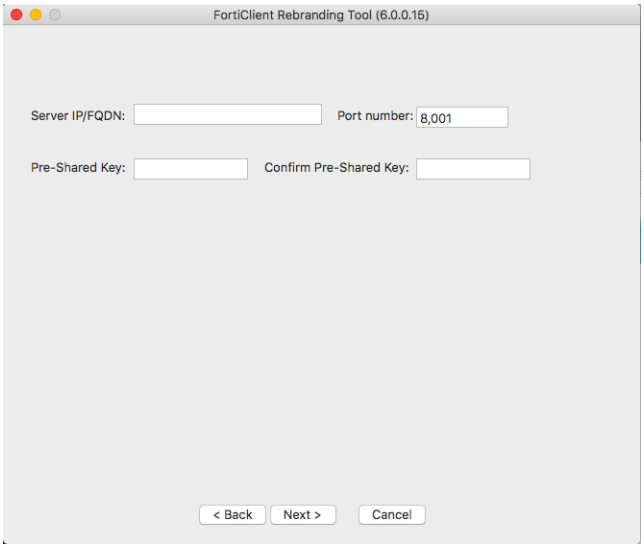
5. Configure the following settings, and click *Start*:



Features to Install		
	Security Fabric Agent	Selected by default to support Fortinet Security Fabric. FortiClient Telemetry is always installed to support integration of FortiClient into the Security Fabric as follows: • Participate in compliance • Send user ID, avatar and email address to FortiGate • Be managed by EMS Along with the Vulnerability Scan component (also included in this agent), this provides the Security Fabric administrators an overview of the state of the endpoint. Clear the checkbox to exclude the *Compliance* tab and *Vulnerability Scan* tab from the FortiClient installation file.
	Secure Remote Access	Select to include SSL and IPsec VPN modules in the FortiClient installation file.
	Additional Security Features	Select to include one or more of the following modules in the FortiClient installation file: • AntiVirus • Web Filtering • Single Sign On • Application Firewall
Options		

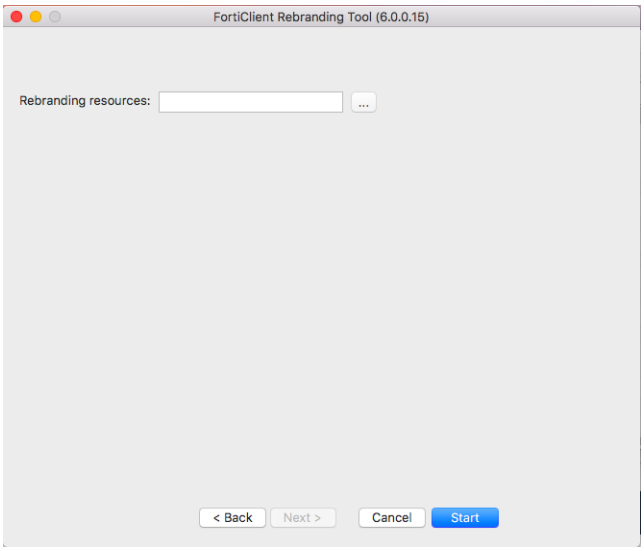
Enable Software Update	Select to enable FortiClient software updates via FortiGuard Distribution Network on endpoints. This option is disabled when rebranding FortiClient. This option is also disabled when using trial mode.
Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator.

6. If you selected the *Configure Single Sign-On mobility agent* checkbox, the *Single Sign-On Mobility Agent Settings* page displays. Configure the following settings:



Server IP/FQDN	Enter the FortiAuthenticator server's IP address or FQDN.
Port number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

7. Select *Next* to continue.
8. In the *Rebranding resources* field, select the directory that contains the rebranded resources, such as graphical elements.



To rebrand elements such as the product name and company website URL, edit the rebrand_text.plist file as desired. See Rebranding FortiClient on page 15.

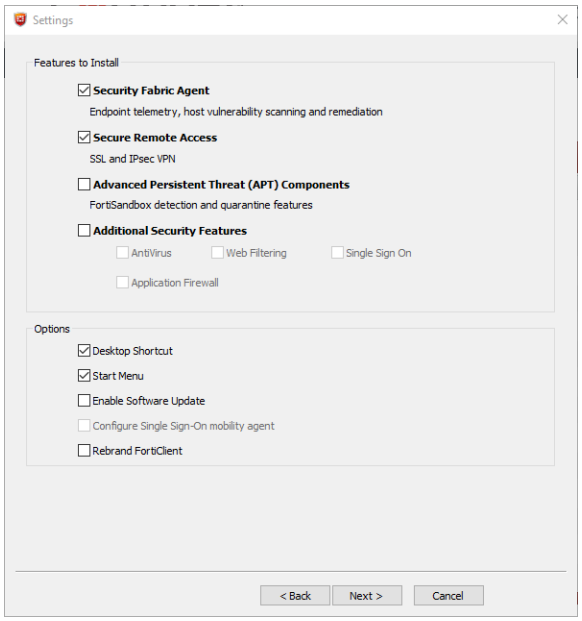
9. Click *Start*.
10. Click *Done*. You can now deploy the repackaged FortiClient `.dmg` file to your Mac OS X systems.

Rebranding FortiClient

You can rebrand FortiClient (Windows) and FortiClient (Mac OS X) using the FortiClient Rebranding Tool.

Rebranding FortiClient (Windows)

The FortiClient Rebranding Tool can be used to create custom FortiClient MSI installers with various combinations of features. The customized MSI installer generated may be used to install FortiClient on all supported platforms using Active Directory. A FortiClient setup executable file is also generated for manual distribution.



Under Options, you can select to enable software updates, configure the single sign-on mobility agent, and rebrand FortiClient. Rebranding allows you to edit various UI elements including graphics.

When replacing files in the resource folder, the replacement file should be the same file type and dimensions. Icons (`.ico`) are a special case. The `Main_icon.ico` file for example, is a composite file of multiple icons. The operating system picks the appropriate icon size from this file for the context in which the icon is being displayed.

Rebranding elements:

Element	Where used	Default value
Product Name	Setup Wizard header and body, File directory name in Installer Company Name file folder, engine/signature update bubble messages.	FortiClient
Company Name	File directory name in Program Files.	Fortinet
Manufacturer Name		Fortinet Inc
Company Website URL	*Help* > *About* > *Copyright* page	http://www.fortinet.com
Company Website Text	*Help* > *About* > *Copyright* page	www.fortinet.com
Feedback Email	*Help* > *About* > *Copyright* page, Send Feedback	forticlient-feedback@fortinet.com
Feedback Email Text	*Help* > *About* > *Copyright* page, Send Feedback	forticlient-feedback@fortinet.com
Technical Documentation Link	*Help* > *Technical Documentation*	http://docs.fortinet.com/fclnt.html

Element	Where used	Default value
Technical Documentation Link Text	*Help > Technical Documentation*	&Technical Documentation
Knowledge Base Link	Link used by Knowledge Base text Leave this field blank to omit the field in the console.	http://kb.fortinet.com
Knowledge Base Link Text	Help menu option Leave this field blank to omit the field in the console.	Fortinet Knowledge Base

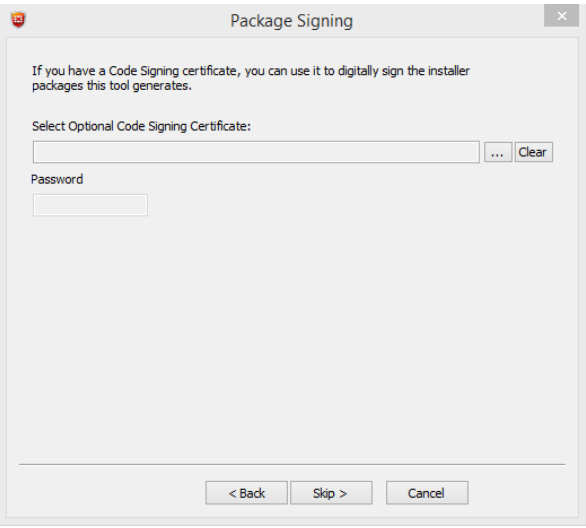
Resources folder elements:

Resource	Where used	File type	Width	Height	Bit depth
About_red_ shield_logo.png		PNG File (.png)	43 pixels	43 pixels	32
Advertisement_ ad_0.png	Dashboard advertisement banner	PNG File (.png)	628 pixels	66 pixels	32
Advertisement_ ad_1.png	Dashboard advertisement banner	PNG File (.png)	628 pixels	66 pixels	32
Advertisement_ ad_2.png	Dashboard advertisement banner	PNG File (.png)	628 pixels	66 pixels	32
Antivirus_AV_ scan_top_ banner_left_ hand_side.png		BMP File (.bmp)	1 pixel	40 pixels	8
Antivirus_AV_ scan_top_ banner_right_ hand_side.png	Banner used in right-click “scan with product name” dialog box	BMP File (.bmp)	440 pixels	40 pixels	8
Common_fgt-not-found-page-bg.png	FortiGate not found page	PNG File (.png)	673 pixels	189 pixels	32
Common_ fortinet-icon.png		PNG File (.png)	79 pixels	79 pixels	32
Common_ registration_ icon.png	FortiGate detected page	PNG File (.png)	85 pixels	85 pixels	32

Resource	Where used	File type	Width	Height	Bit depth
Common_ searching-page-bg.png	Searching for FortiGate page	PNG File (.png)	673 pixels	189 pixels	32
Dashboard_ forticlient_v5_ dashboard_ bg.png	Client console	PNG File (.png)	628 pixels	451 pixels	32
Dashboard_ warning-shield.png	Dashboard warning shield, displayed when antivirus is disabled.	PNG File (.png)	59 pixels	75 pixels	32
Installer_ background.bmp	Setup Wizard background image.	BMP file (.bmp)	491 pixels	312 pixels	8
Installer_ banner.bmp	Setup Wizard banner image on destination page, ready to install page, installing pages.	BMP file (.bmp)	491 pixels	58 pixels	8
Installer_ setup.exe_ icon.ico	Installer setup icon.	ICO File (.ico)	256 pixels	256 pixels	32
LightInstaller_ icon.ico	Light Installer Icon	ICO File (.ico)	32 pixels	32 pixels	32
Main_icon.ico	Shortcut on desktop	ICO file (.ico)	48 pixels	48 pixels	32
Main_logo_ black.ico	Client console header	ICO file (.ico)	32 pixels	32 pixels	32
Tray_Icons_ running.ico	System tray running icon	ICO File (.ico)	16 pixels	16 pixels	32

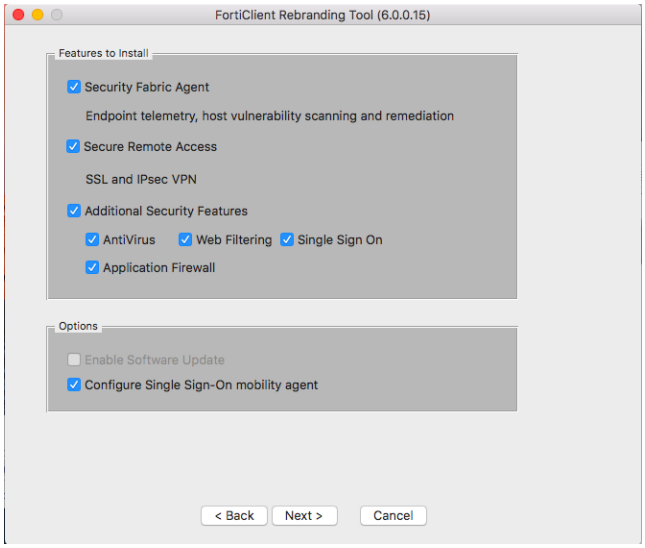
Resource	Where used	File type	Width	Height	Bit depth
Tray_Icons_scan1.ico, Tray_Icons_scan2.ico, Tray_Icons_scan3.ico, Tray_Icons_scan4.ico, Tray_Icons_scan5.ico, Tray_Icons_scan6.ico, Tray_Icons_scan7.ico, Tray_Icons_scan8.ico, Tray_Icons_scan9.ico, Tray_Icons_scan10.ico Tray_Icons_scan11.ico	System tray, these eleven images animate the scanning activity of the tray icon.	ICO File (.ico)	16 pixels	16 pixels	32
Tray_Icons_vpn.ico	System tray VPN icon	ICO File (.ico)	16 pixels	16 pixels	32
VPN_xauth-dialog-logo.png	VPN xAuth dialog logo	PNG File (.png)	88 pixels	100 pixels	32
zzz_rebranding.ini	This file is used by the FortiClient Configurator tool for element/resource mapping.	Configuration settings (.ini)			

When rebranding FortiClient, you can select to digitally sign the installer package using a code signing certificate.

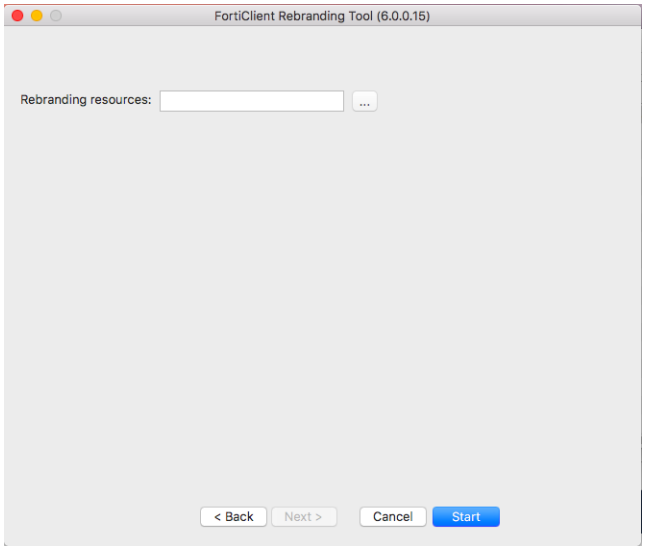


Rebranding FortiClient (Mac OS X)

The FortiClient Rebranding Tool can be used to create custom FortiClient installers with various combinations of features. The customized installer generated may be used to install FortiClient on all supported platforms.



To rebrand FortiClient, in the *Rebranding resources* field, select the directory that contains the rebranded resources, such as graphical elements.



When replacing files in the resource folder, the replacement file should be the same file type and dimensions.

To rebrand FortiClient GUI text, edit the rebrand_text.plist file and enter the desired values.

Element	Where used	Default value
Product Name	Setup Wizard header and body, File directory name in Installer Company Name file folder, engine/signature update bubble messages.	FortiClient
CopyRight	*FortiClient* > *About FortiClient* page	2006-2017 Fortinet Inc. All Rights reserved.
CompanyWebsiteText	*FortiClient* > *About FortiClient* page	www.fortinet.com
CompanyWebsiteURL	*FortiClient* > *About FortiClient* page	http://www.fortinet.com
FortiClientEULA	*FortiClient* > *About FortiClient* page	https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf
TechDocURL	*Help* > *Technical Documentation*	http://docs.fortinet.com/fclnt.html
AdURL1	Dashboard advertisement banner	
AdURL2	Dashboard advertisement banner	
AdURL3	Dashboard advertisement banner	

Resources folder elements:

Resource	Where used	File type	Width	Height
ad_1.png	Dashboard advertisement banner	PNG file (.png)	628 pixels	66 pixels

Resource	Where used	File type	Width	Height
ad_2.png	Dashboard advertisement banner	PNG file (.png)	628 pixels	66 pixels
ad_3.png	Dashboard advertisement banner	PNG file (.png)	628 pixels	66 pixels
ad_close_hover.png	Dashboard advertisement banner	PNG file (.png)	13 pixels	13 pixels
ad_close.png	Dashboard advertisement banner	PNG file (.png)	13 pixels	13 pixels
ad_install_all_security.png	Dashboard advertisement banner	PNG file (.png)	628 pixels	66 pixels
Alert-Anti-Virus.png		PNG file (.png)	21 pixels	21 pixels
Alert-App-Firewall.png		PNG file (.png)	21 pixels	21 pixels
Alert-Parental-Control.png		PNG file (.png)	21 pixels	21 pixels
Alert-Remote-Access.png		PNG file (.png)	21 pixels	21 pixels
Alert-Vulnerability-Scan.png		PNG file (.png)	21 pixels	21 pixels
Alert-Web-Filter.png		PNG file (.png)	21 pixels	21 pixels
Alerts_green.png		PNG file (.png)	14 pixels	14 pixels
alerts.png		PNG file (.png)	14 pixels	14 pixels
Anti-Virus-Disable.png		PNG file (.png)	38 pixels	36 pixels
Anti-Virus-Enable.png		PNG file (.png)	38 pixels	36 pixels
Anti-Virus-light-blue.png		PNG file (.png)	38 pixels	36 pixels
antivirus-icon.png		PNG file (.png)	32 pixels	32 pixels
Application-Firewall_light-blue.png		PNG file (.png)	38 pixels	36 pixels
bigicon_alert.png		PNG file (.png)	80 pixels	80 pixels
biglock.png		PNG file (.png)	720 pixels	720 pixels
bluedot.png		PNG file (.png)	6 pixels	6 pixels
btn_blue_142x36_hover.png		PNG file (.png)	142 pixels	36 pixels

Resource	Where used	File type	Width	Height
btn_blue_142x36_normal.png		PNG file (.png)	142 pixels	36 pixels
btn_go_disabled.png		PNG file (.png)	18 pixels	18 pixels
btn_go_hover.png		PNG file (.png)	18 pixels	18 pixels
btn_go_normal.png		PNG file (.png)	18 pixels	18 pixels
Bytes-Received.png		PNG file (.png)	16 pixels	16 pixels
Bytes-Sent.png		PNG file (.png)	16 pixels	16 pixels
ColumnMinus.png		PNG file (.png)	22 pixels	27 pixels
ColumnMinusGray.png		PNG file (.png)	22 pixels	27 pixels
ColumnMinusHover.png		PNG file (.png)	22 pixels	27 pixels
ColumnNote.png		PNG file (.png)	23 pixels	27 pixels
ColumnNoteGray.png		PNG file (.png)	23 pixels	27 pixels
ColumnNoteHover.png		PNG file (.png)	23 pixels	27 pixels
ColumnPlus.png		PNG file (.png)	22 pixels	27 pixels
ColumnPlusHover.png		PNG file (.png)	22 pixels	27 pixels
Compliance_disabled.png		PNG file (.png)	38 pixels	36 pixels
Compliance_enabled.png		PNG file (.png)	38 pixels	36 pixels
Compliance_light-blue.png		PNG file (.png)	38 pixels	36 pixels
compliance-warning.png		PNG file (.png)	35 pixels	33 pixels
compliance.png		PNG file (.png)	35 pixels	35 pixels
cross_icon.png		PNG file (.png)	16 pixels	16 pixels
dashboard_ipsecvpn.png		PNG file (.png)	112 pixels	125 pixels
dashboard_sslvpn.png		PNG file (.png)	112 pixels	125 pixels
device.png		PNG file (.png)	70 pixels	52 pixels
disable.png		PNG file (.png)	31 pixels	31 pixels
disicons_no.png		PNG file (.png)	14 pixels	14 pixels
disicons_registered_ offline.png		PNG file (.png)	14 pixels	14 pixels
disicons_registered.png		PNG file (.png)	14 pixels	14 pixels
disicons_tick.png		PNG file (.png)	14 pixels	14 pixels

Resource	Where used	File type	Width	Height
disicons_unregistered.png		PNG file (.png)	14 pixels	14 pixels
down.png		PNG file (.png)	10 pixels	10 pixels
Duration.png		PNG file (.png)	16 pixels	16 pixels
edit_blue.png		PNG file (.png)	10 pixels	10 pixels
edit_grey.png		PNG file (.png)	10 pixels	10 pixels
email_info.png		PNG file (.png)	16 pixels	16 pixels
ems_icon.png		PNG file (.png)	16 pixels	16 pixels
Enable.png		PNG file (.png)	31 pixels	31 pixels
Exclusion-List-icon.png		PNG file (.png)	31 pixels	31 pixels
Feature-Disabled.png		PNG file (.png)	16 pixels	16 pixels
Feature-enabled.png		PNG file (.png)	16 pixels	16 pixels
file_icon.png		PNG file (.png)	32 pixels	32 pixels
firewall-pre.png		PNG file (.png)	16 pixels	16 pixels
FortiClient_bg.png		PNG file (.png)	628 pixels	451 pixels
fortiClient_software.png		PNG file (.png)	16 pixels	16 pixels
FortiClientConnect_On.icns		ICNS file (.icns)	128 pixels	128 pixels
FortiClientConnect.icns		ICNS file (.icns)	128 pixels	128 pixels
FortiClientVPNOnly_bg.png		PNG file (.png)	628 pixels	451 pixels
fortiheartbeat.png		PNG file (.png)	16 pixels	16 pixels
fw_icon_status.png		PNG file (.png)	31 pixels	31 pixels
fw-disabled.png		PNG file (.png)	38 pixels	36 pixels
fw-enabled.png		PNG file (.png)	38 pixels	36 pixels
gear_icon.png		PNG file (.png)	16 pixels	16 pixels
google_white.png		PNG file (.png)	14 pixels	18 pixels
google.png		PNG file (.png)	14 pixels	18 pixels
Green-shield.png		PNG file (.png)	73 pixels	86 pixels
icon_alert.png		PNG file (.png)	14 pixels	14 pixels
icon_critical-vuln.png		PNG file (.png)	31 pixels	31 pixels
icon_no.png		PNG file (.png)	14 pixels	14 pixels

Resource	Where used	File type	Width	Height
icon_scan.png		PNG file (.png)	31 pixels	31 pixels
icon_small_blue_shield.png		PNG file (.png)	15 pixels	15 pixels
icon_small_grey_shield.png		PNG file (.png)	15 pixels	15 pixels
icon_vuln-detected.png		PNG file (.png)	31 pixels	31 pixels
inbound_block.png		PNG file (.png)	12 pixels	12 pixels
IPSec-Connected-icon.png		PNG file (.png)	71 pixels	50 pixels
item_selected.png		PNG file (.png)	49 pixels	30 pixels
item_unselected.png		PNG file (.png)	50 pixels	29 pixels
LinkedIn_white.png		PNG file (.png)	14 pixels	18 pixels
LinkedIn.png		PNG file (.png)	14 pixels	18 pixels
little_graywarnning.png		PNG file (.png)	20 pixels	20 pixels
lock_icon.png		PNG file (.png)	16 pixels	16 pixels
logging-icon.png		PNG file (.png)	32 pixels	32 pixels
macos.png		PNG file (.png)	28 pixels	36 pixels
monitor.png		PNG file (.png)	16 pixels	16 pixels
nav_button_help_hover.png		PNG file (.png)	30 pixels	28 pixels
nav_button_help.png		PNG file (.png)	30 pixels	28 pixels
nav_chevron.png		PNG file (.png)	20 pixels	28 pixels
non-compliance.png		PNG file (.png)	31 pixels	31 pixels
off-net.png		PNG file (.png)	32 pixels	11 pixels
on-net.png		PNG file (.png)	32 pixels	11 pixels
outbound_block.png		PNG file (.png)	12 pixels	12 pixels
Parental-Control_light_ bue.png		PNG file (.png)	38 pixels	36 pixels
parental-control-disabled.png		PNG file (.png)	38 pixels	36 pixels
parental-control-enabled.png		PNG file (.png)	38 pixels	36 pixels
phone_info.png		PNG file (.png)	16 pixels	16 pixels
refresh_normal_bg.png		PNG file (.png)	22 pixels	27 pixels
refresh_pressed_bg.png		PNG file (.png)	22 pixels	27 pixels

Resource	Where used	File type	Width	Height
reg_close_icon.png		PNG file (.png)	10 pixels	10 pixels
reg_refresh_icon.png		PNG file (.png)	9 pixels	12 pixels
registration-pre.png		PNG file (.png)	32 pixels	32 pixels
Remote-Access_disabled.png		PNG file (.png)	38 pixels	36 pixels
Remote-Access_enabled.png		PNG file (.png)	38 pixels	36 pixels
Remote-Access_light-blue.png		PNG file (.png)	38 pixels	36 pixels
salesforce_white.png		PNG file (.png)	14 pixels	18 pixels
salesforce.png		PNG file (.png)	14 pixels	18 pixels
scan-complete-nothreats2.png		PNG file (.png)	139 pixels	99 pixels
scan-complete2.png		PNG file (.png)	139 pixels	99 pixels
Scan-now.png		PNG file (.png)	19 pixels	19 pixels
scan-schedule.png		PNG file (.png)	31 pixels	31 pixels
scanning.gif		GIF file (.gif)	113 pixels	99 pixels
security-alert.png		PNG file (.png)	120 pixels	138 pixels
selected_category_background.png		PNG file (.png)	192 pixels	34 pixels
Selected-tab_bottom.png		PNG file (.png)	228 pixels	87 pixels
Selected-tab.png		PNG file (.png)	229 pixels	72 pixels
severity_1.png		PNG file (.png)	13 pixels	13 pixels
severity_2.png		PNG file (.png)	13 pixels	13 pixels
severity_3.png		PNG file (.png)	13 pixels	13 pixels
severity_4.png		PNG file (.png)	13 pixels	13 pixels
severity_5.png		PNG file (.png)	13 pixels	13 pixels
Shield_warning.png		PNG file (.png)	31 pixels	31 pixels
Sites-Blocked_icon.png		PNG file (.png)	16 pixels	16 pixels
small_stop_icon.png		PNG file (.png)	28 pixels	28 pixels
specify_white.png		PNG file (.png)	14 pixels	18 pixels
specify.png		PNG file (.png)	14 pixels	18 pixels

Resource	Where used	File type	Width	Height
SSL-Connected-icon.png		PNG file (.png)	71 pixels	50 pixels
system-compliant.png		PNG file (.png)	16 pixels	16 pixels
TableColumnBackground.png		PNG file (.png)	1 pixel	28 pixels
threats-quarantined-0.png		PNG file (.png)	31 pixels	31 pixels
tick.png		PNG file (.png)	16 pixels	16 pixels
uncheck.png		PNG file (.png)	16 pixels	16 pixels
unlock_icon.png		PNG file (.png)	16 pixels	16 pixels
Unregister_small.png		PNG file (.png)	16 pixels	16 pixels
Unregister.png		PNG file (.png)	46 pixels	46 pixels
unregistered_device_ blue.png		PNG file (.png)	41 pixels	10 pixels
unregistered_device_ white.png		PNG file (.png)	41 pixels	10 pixels
Up.png		PNG file (.png)	10 pixels	10 pixels
Update-now.png		PNG file (.png)	19 pixels	19 pixels
User-offline_small.png		PNG file (.png)	16 pixels	16 pixels
User-offline.png		PNG file (.png)	32 pixels	32 pixels
User-online_small.png		PNG file (.png)	16 pixels	16 pixels
user.png		PNG file (.png)	32 pixels	32 pixels
View-Gateway-IP-List.png		PNG file (.png)	16 pixels	16 pixels
vul_scan.png		PNG file (.png)	14 pixels	14 pixels
vul-disabled.png		PNG file (.png)	16 pixels	16 pixels
vul-enabled.png		PNG file (.png)	38 pixels	36 pixels
Vulnerabilities-found_ icon.png		PNG file (.png)	16 pixels	16 pixels
Vulnerability-Scan_light-blue.png		PNG file (.png)	38 pixels	36 pixels
warning_icon.png		PNG file (.png)	16 pixels	16 pixels
warning-shield.png		PNG file (.png)	73 pixels	86 pixels
Web-Filter_disabled.png		PNG file (.png)	38 pixels	36 pixels

Resource	Where used	File type	Width	Height
Web-Filter_enabled.png		PNG file (.png)	38 pixels	36 pixels
Web-Filter_light-blue.png		PNG file (.png)	38 pixels	36 pixels
Web-Filter.png		PNG file (.png)	31 pixels	31 pixels
webfilter-pre.png		PNG file (.png)	32 pixels	32 pixels
wf_action_revised_gray.png		PNG file (.png)	16 pixels	16 pixels
wf_action_revised.png		PNG file (.png)	16 pixels	16 pixels
wf_action.allow_gray.png		PNG file (.png)	16 pixels	16 pixels
wf_action.allow.png		PNG file (.png)	16 pixels	16 pixels
wf_action.block_gray.png		PNG file (.png)	16 pixels	16 pixels
wf_action.block.png		PNG file (.png)	16 pixels	16 pixels
wf_action.monitor_gray.png		PNG file (.png)	16 pixels	16 pixels
wf_action.monitor.png		PNG file (.png)	16 pixels	16 pixels
wf_action.warning_gray.png		PNG file (.png)	16 pixels	16 pixels
wf_action.warning.png		PNG file (.png)	16 pixels	16 pixels

Deploying custom FortiClient installation packages

This section includes information about deploying FortiClient (Windows) installation packages and FortiClient (OS X) installation files.

Deploying FortiClient (Windows) installation packages

After the FortiClient Rebranding Tool generates the custom installation packages, you can use the custom installation packages to deploy FortiClient (Windows) software manually or using Active Directory. Both options can be found in the *.../FortiClient_packaged* directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

If you are using Active Directory to deploy FortiClient (Windows), you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

For manual distribution, use the `.exe` file in the *.../ManualDistribution* folder.

Deploying FortiClient (OS X) installation files

After the FortiClient Rebranding Tool generates the custom installation file (`.dmg` file), you can use the custom installation file to deploy FortiClient (OS X) software.